

### **REMARKS**

The Office Action dated August 10, 2006 has been received and carefully noted. The above amendments to the claims and the following remarks are submitted as a full and complete response thereto.

Claims 14, 20-23, 25, 27-29 and 31-39 are amended to more particularly point out and distinctly claim the subject matter of the invention and to correct typographical informalities. No new matter is added. Claims 2-14, 16, 17, 19-29 and 31-39 are respectfully submitted for consideration.

The Office Action objected to claims 36-39 as being substantial duplicates of claims 21, 31, 33 and 34 respectively. As discussed in MPEP 706.03(k) Applicants have the right to claim an invention in a reasonable number of ways, even if there is a mere difference in scope. In the present application, the Applicant respectfully submits that claims 36-39 are clearly recited in means-plus-function terminology which differs in scope from claims 21, 31, 33 and 34. Therefore, claims 36-39 are not substantial duplicates as alleged in the Office Action.

Further, MPEP 706.03(k) also states that “it is proper after allowing one claim to object to the other claim under 37 C.F.R. as being a substantial duplicate of the allowed claims.” (underline added). Thus, in the present case, since none of the claims have been indicated to be allowed in the Office Action, this objection is premature.

Based at least on the above, Applicant respectfully requests withdrawal of the objection to claims 36-39.

The Office Action rejected claims 2-14, 16, 17, 19-29 and 31-39 as being obvious over US Patent No. 6,577,865 to Dikmen et al. (Dikmen), in view of US Patent No. 6,771,597 (Makansi et al. (Makansi)). The Office Action took the position that Dikmen disclosed all of the features recited in these claims except a first network element generates fake packets to be transmitted with said intercepted data packets and the fake packets are transmitted from said first network element to said interception gateway element, wherein said fake packets are transmitted at random or triggered at any passing packet such that the total load of intercepted and fake packets transmitted to said interception gateway is constant. The Office Action asserted that Makansi disclosed the features of the a first network element generates fake packets to be transmitted with said intercepted data packets and the fake packets are transmitted from said first network element to said interception gateway element, wherein said fake packets are transmitted at random or triggered at any passing packet. The Office Action took Official Notice that the total load of intercepted and fake packets is constant. Applicant respectfully submits that the cited references, taken individually or in combination, fail to disclose or suggest all of the features recited in any of the pending claims.

Claim 14, from which claims 2-13, 16 and 17 depend, is directed to an interception method for performing a lawful interception in a packet network. A first network element includes an interception function to intercept data packets is provided. The interception function is controlled by an interception control means implemented in a second network element. An intercepted data packet is transmitted from the first network

element via the packet network to an interception gateway element providing an interface to at least one intercepting authority. The first network element generates fake packets to be transmitted with the intercepted data packets and the fake packets are transmitted from the first network element to the interception gateway element. The fake packets are transmitted at random or triggered at any passing packet, such that the total load of intercepted and fake packets transmitted to the interception gateway element is constant.

Claim 21, from which claims 19-20, 22-29 and 32 depend, is directed to an interception system. A first network element includes an interception function to intercept data packets and comprising a transmitting unit configured to transmit an intercepted data packet to the packet network. An interception control unit is implemented in a second network element and configured to control the interception function. An interception gateway element includes a receiving unit configured to receive the intercepted data packet and an interface unit configured to provide an interface to at least one intercepting authority. The first network element further includes a generating unit that is configured to generate fake packets to be transmitted with the intercepted data packets. The transmitting unit is further configured to transmit the fake packets at random or triggered at any passing packet, such that the total load of intercepted and fake packets transmitted to the interception gateway element is constant. The interception system is configured to perform the lawful interception in the packet network.

Claim 33 is directed to a network element for a packet network. An interception unit is configured to intercept a data packet received from the packet network. A

transmitting unit is configured to transmit the intercepted data packet via the packet network to an interception gateway element. The interception unit is controlled by an interception control unit configured in another network element. The network element further includes a generating unit configured to generate fake packets to be transmitted with the intercepted data packets. The fake packets are transmitted from the network element to the interception gateway element and are transmitted at random or triggered at any passing packet, such that the total load of intercepted and fake packets transmitted to the interception gateway element is constant.

Claim 34, from which claim 35 depends, is directed to an interception gateway element for an interception system of a packet network. A receiving unit is configured to receive an intercepted data packet via said packet network from a network element having an interception function. An interface unit is configured to provide an interface to an intercepting authority. A memory unit is configured to store received intercepted data packets before supplying them to the interface unit. The interception gateway element includes a decryption unit configured to remove an encryption of the received intercepted data packets, an extraction unit configured to extract intercepted data packets from fake data packets, and an adding unit configured to add a time information to the received intercepted data packets before storing them in the memory.

Claim 36 is directed to an interception system. A first network element includes an interception function for intercepting data packets. The first network element further includes a transmitting means for transmitting an intercepted data packet to said packet

network. An interception control means is implemented in a second network element, for controlling the interception function. An interception gateway element includes a receiving means for receiving said intercepted data packet and an interface unit for providing an interface to at least one intercepting authority. The first network element further includes a generating means for generating fake packets to be transmitted with said intercepted data packets. The transmitting means is further configured for transmitting said fake packets at random or triggered at any passing packet, such that the total load of intercepted and fake packets transmitted to the interception gateway element is constant. The interception system is configured for performing a lawful interception in a packet network.

Claim 37 is directed to an interception system. A first network element includes an interception function for intercepting data packets and a transmitting means for transmitting an intercepted data packet to said packet network. An interception control means implemented in a second network element and configured for controlling the interception function. An interception gateway element having a receiving means for receiving said intercepted data packet and an interface means for providing an interface to at least one intercepting authority, wherein said interception gateway element comprises a memory means for storing received intercepted data packets before supplying them to the interface means. The interception gateway element includes a decryption means for removing an encryption of the received intercepted data packets, an extraction means for extracting intercepted data packets from fake data packets, and a

means for adding a time information to said received intercepted data packets before storing them in the memory means. The transmitting means transmits the fake packets at random or triggered at any passing packet, such that the total load of intercepted and fake packets transmitted to the interception gateway element is constant. The interception system is configured for performing lawful interception in the packet network.

Claim 38 is directed to a network element for a packet network. The network element includes an interception means for intercepting a data packet received from the packet network. A transmitting means transmits the intercepted data packet via the packet network to an interception gateway element. The interception means is controlled by an interception control means in another network element. The network element further includes means for generating fake packets to be transmitted with the intercepted data packets. The fake packets are transmitted from the network element to the interception gateway element. The fake packets are transmitted at random or triggered at any passing packet, such that the total load of intercepted and fake packets transmitted to the interception gateway element is constant.

Claim 39 is directed to an interception gateway element. A receiving means receives an intercepted data packet via the packet network from a network element having an interception function. An interface means provides an interface to an intercepting authority. A memory means stores received intercepted data packets before supplying them to the interface means. The interception gateway element includes a

decryption means for removing an encryption of the received intercepted data packets, an extraction means for extracting intercepted data packets from fake data packets and a adding means for adding a time information to the received intercepted data packets before storing them in the memory means unit.

Applicant respectfully submits that each of the pending claims recite features that are neither disclosed nor suggested in any of the cited references.

Dikmen is directed to a system for the intercept of wireless communications wherein a HLR of a wireless communications system includes one or more flags associated with each subscriber, and the HLR notifies an intercept server each time a call event is detected in the HLR for a subscriber under surveillance as indicated by the flags. The intercept server includes a Gateway Delivery Function module and one or more Delivery Function modules, wherein the Gateway Delivery Function module provisions the Delivery Function modules depending on the location of the subscriber, to deliver call content or data from an MSC to a collection function operated by a law enforcement agency. Non-call associated data is also provided to a Delivery Function module for delivery to a Collection Function.

Makansi is directed to a method and apparatus for transmitting messages. Although it does not specifically relate to lawful interception, it deals with message transmission in terms of preventing interception. According to Makansi, a message (which might also represent an intercepted stream of data packets, not admitted) is split into several packets and dummy data are added to one or more of the packets (See

column 7, lines 25 to 28 of Makansi). In addition, Makansi teaches that packets (payload) can be interspersed with dummy packets. The dummy packets will be transmitted with the packets of the message in order to make it more difficult for an unauthorized person to determine the contents of the message (See column 7, lines 35 to 38 of Makansi).

Applicant respectfully submits that the cited references fail to disclose suggest all of the features recited in the above claims because Makansi and the Official Notice fail to cure the admitted deficiencies of Dikmen. More specifically, the cited references fail to disclose or suggest at least the feature that the fake packets are transmitted at random or triggered at any passing packet such that the total load of intercepted and fake packets transmitted to said interception gateway is constant, as recited in claim 14 and similarly recited in claims 21 and 33, 34 and 36-39.

Applicants respectfully traverse the Official Notice taken in the Office Action regarding the US Patent No. 4,797,880 to Bussey Jr. (Bussey), in which the Office Action cites as evidence that the total load of intercepted and fake packets that are transmitted to the interception gateway element is constant.

As discussed in the Response dated July 6, 2006, Bussey is directed to a non-blocking, self-routing packet switch. As described in Bussey, fake, place-holding packets are used to insure that during each packet switch cycle a packet is routed from each input port to each output port. However, Applicants submits that Bussey fails to mention, disclose or suggest, that the total load of intercepted and fake packets is constant. Further, the Office Action asserted in its Official Notice that “in a general case network



elements function optimally when traffic is constant” is well-known in the art. Applicant respectfully traverses this assertion. For example, in networks that are designed to utilized variable bit-rate traffic (VBR), according to the Office Action’s assertion, VBR traffic networks would not function optimally, which one skilled in the art would recognize as not being a true statement.

Applicant respectfully submits that because claims 2-13, 16, 17, 19, 20, 22-29 and 31, 32, 35 depend from claims 14, 21 and 34, these claims are allowable at least for the same reasons as claims 14, 21, and 34 as well as for the additional features recited in these dependent claims.

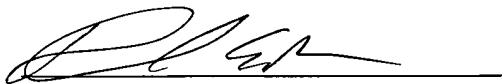
Based at least on the above, Applicants respectfully submit that the cited references fail to disclose or suggest all of the features recited in claims 2-14, 16, 17, 19-29 and 31-39. Accordingly, withdrawal of the rejection of claims 2-14, 16, 17, 19-29 and 31-39 under 35 U.S.C. 103(a) is respectfully requested.

Applicant respectfully requests that each of claims 2-14, 16, 17, 19-29 and 31-39 be allowed and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant’s undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



David E. Brown  
Registration No. 51,091

**Customer No. 32294**  
SQUIRE, SANDERS & DEMPSEY LLP  
14<sup>TH</sup> Floor  
8000 Towers Crescent Drive  
Tysons Corner, Virginia 22182-2700  
Telephone: 703-720-7800  
Fax: 703-720-7802

DEB:jkm